

### **Welcome to the PIA for FY 2010!**

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

#### **Directions:**

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: <http://vawww.privacy.va.gov/PIA.asp>

#### **Roles and Responsibilities:**

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and reviewing and approving the PIA before submission to the Privacy Service.

**Definition of PII (Personally Identifiable Information)**

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

**Macros Must Be Enabled on This Form**

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

## (FY 2010) PIA: System Identification

---

Program or System Name: Captain James A Lovell, Federal Health Care Center-  
Inter-Agency Services

OMB Unique System / Application / Program

Identifier (AKA: UPID #): JIF# 00-001

Description of System / Application / Program: The Captain James A. Lovell FHCC-IAS provides the ability for staff at the Captain JAL FHCC to provide timely and appropriate health care services to Veterans and Active-Duty Department of Defense (DoD) service members and their dependants. Furthermore, the implementation of JAL FHCC-IAS provides interoperability of Health Information records between the Department of Veterans Affairs (DVA) and the Department of Defense, using a single point of entry. The Patient Registration Application is the primary graphical user interface (GUI) that supports a joint Patient Registration process. JALFHCC-IAS is designed to run continuously, supporting the VA and DoD Health Information Management Systems, within the JALFHCC's computing environment.

---

Facility Name: Captain James A Lovell, Federal Health Care Center

Title:	Name:	Phone:
Privacy Officer:	Sheila Merrier	224-610-3383
Information Security Officer:	John Rinkema	224-610-3805
Chief Information Officer:	Paul Lam	224-610-5700

Person Completing Document:	Mayra Acevedo-Negron	561-422-1290
Other Titles:	n/a	
Other Titles:	n/a	
Other Titles:		
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	n/a	
Date Approval To Operate Expires:	n/a	

---

What specific legal authorities authorize this program or system:	Section 1635 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2008(P.L. 110-181) mandated the establishment of a DoD/VA IPO to act as a single point of accountability for DoD and VA.
What is the expected number of individuals that will have their PII stored in this system:	1-999999
Identify what stage the System / Application / Program is at:	Development/Acquisition
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	10/2010
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	No
Date of Report (MM/YYYY):	n/a

**Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form**

- ☐ Have any changes been made to the system since the last PIA?
- ☒ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

**If there is no Personally Identifiable Information on your system , please skip to TAB 12. ( See Comment for Definitio**

---

---

Email:  
[sheila.merrier2@va.gov](mailto:sheila.merrier2@va.gov)  
[john.rinkema@va.gov](mailto:john.rinkema@va.gov)  
[paul.lam@va.gov](mailto:paul.lam@va.gov)

[mayra.acevedo-negron@va.gov](mailto:mayra.acevedo-negron@va.gov)

n.

or others performing work

· identifier, symbol, or

n of PII)

## (FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

24VA19

2. Name of the System of Records:

Vista Legacy

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

***(Please Select Yes/No)***

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

## (FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)				
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information				
Criminal Record Information				
Guardian Information	ALL		All	All
Education Information	ALL		All	All
Benefit Information	ALL		All	All
Other (Explain)	ALL		All	All

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	Patient Registration Information
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	Patient Registration Information
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	Patient Registration Information
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Patient Registration Information
Criminal Record Information	No			

Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory	Patient Registration Information
Education Information	No			
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Patient Registration Information
Other (Explain)	No			
Other (Explain)				
Other (Explain)				

### (FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA	Yes	benefits	Both PII & PHI	VA Directive 6500
Other Veteran Organization		No		N/A	
Other Federal Government Agency	Dept of Defense (DoD)	Yes	Patient Registration Application; lab,pharmacy, radiology, and consults orders portability	Both PII & PHI	MOU/ISA dated June 21, 2005 signed by the VA and DOD
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System		No		N/A	
Other Project / System		No			
Other Project / System		No			

### (FY 2010) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: VA's VISTA and CPRS and DOD's CHCS/AHLTA

Per responses in Tab 4, does the system gather information from an individual? Yes

If information is gathered from an individual, is the information provided:

- ☒ Through a Written Request
- ☒ Submitted in Person
- ☒ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down? Yes

### (FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? Yes

- ☐ Drug/Alcohol Counseling    ☐ Mental Health    ☐ HIV  
☒ Research    ☐ Sickle Cell    ☐ Other (Please Explain)

if yes, please check all that apply:

Describe process for authorizing access to this data.

He/she will be authenticated by certificate OR user name and password that is assigned for the Citrix session. Once authenticated by the credentials, the Citrix manager prompts an access id and verification code that gets stored with the certificate/user name after the first log-in. (ideally, one key chain for VA and one key chain for DoD). There is a requirement for a smart card implementation (i.e. CAC or PIV) at North Chicago.

Answer:

## (FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer:

Manual collection of data elements

How is data checked for completeness?

Answer:

The Data receives a manual quality review by one or more staff reviewing data against present standard assurance.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

Quality reviews by staff members by using present quality indicators

How is new data verified for relevance, authenticity and accuracy?

Answer:

Data receives a manual quality review by one or more staff reviewing data against present standards.

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

## (FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer:

Refer to RCS-10-1

Destroy/Delete 75 years after the last episode of patient care.

Explain why the information is needed for the indicated retention period?

Answer:

For patient health care

What are the procedures for eliminating data at the end of the retention period?

Answer:

Unless retrieved, records transferred to a storage facility will be destroyed after expiration of their retention requirements. However, the transferring facility will be notified prior the destruction of the records. The transferring facility will be notified by the storage facility that the records will become eligible for destruction in the near future. If the records are to be retained beyond their destruction date, the transferring facility must notify the storage facility that the records are to be retained beyond the destruction date. If the storage facility is not notified, the records will be destroyed after their retention periods have expired.

Where are these procedures documented?

Answer:

VA Directive & Handbook 6300.1, VHA Memo 10-2003-001 and NARA regulations, Title 36, Code of Federal Regulations, Part 1228, Disposition of Federal Records, and VA Handbook 6300.1, Chapter 6, Records Disposition Program.

---

How are data retention procedures enforced?

Answer:

Local records management officer is available for guidance

---

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

---

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

NARA regulations, Title 36, Code of Federal Regulations, Part 1228, Disposition of Federal Records, and VA Handbook 6300.1, Chapter 6, Records Disposition Program.

---

### (FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

---

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

---

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why: Answer:	
Is adequate physical security in place to protect against unauthorized access?	Yes
If 'No' please describe why: Answer:	
Explain how the project meets IT security requirements and procedures required by federal law. Answer:	
The JALFHCC-IAS v 1.0 System Security Plan (SSP) is a formal living document that provides an overview of the security requirements and describes the security controls in place to meet those requirements. The SSP is required for Certification and Accreditation of an information system per FISMA and Federal Regulations. Additionally, the JALFHCC-IAS Security Team was given guidance by the VA Office of Cyber and Information Security (OCIS) to follow the National Institute of Standards and Technology, NIST 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems" methodology for the Certification and Accreditation (C&A) of JALFHCC-IAS.	

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- |  |   |
|--|---|
| <input type="checkbox"/> Air Conditioning Failure                        | <input type="checkbox"/> Hardware Failure                                 |
| <input type="checkbox"/> Chemical/Biological Contamination               | <input checked="" type="checkbox"/> Malicious Code                        |
| <input type="checkbox"/> Blackmail                                       | <input type="checkbox"/> Computer Misuse                                  |
| <input type="checkbox"/> Bomb Threats                                    | <input checked="" type="checkbox"/> Power Loss                            |
| <input checked="" type="checkbox"/> Cold/Frost/Snow                      | <input checked="" type="checkbox"/> Sabotage/Terrorism                    |
| <input type="checkbox"/> Communications Loss                             | <input type="checkbox"/> Storms/Hurricanes                                |
| <input type="checkbox"/> Computer Intrusion                              | <input type="checkbox"/> Substance Abuse                                  |
| <input type="checkbox"/> Data Destruction                                | <input checked="" type="checkbox"/> Theft of Assets                       |
| <input type="checkbox"/> Data Disclosure                                 | <input type="checkbox"/> Theft of Data                                    |
| <input type="checkbox"/> Data Integrity Loss                             | <input type="checkbox"/> Vandalism/Rioting                                |
| <input type="checkbox"/> Denial of Service Attacks                       | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) |
| <input type="checkbox"/> Earthquakes                                     | <input checked="" type="checkbox"/> Burglary/Break In/Robbery             |
| <input type="checkbox"/> Eavesdropping/Interception                      | <input type="checkbox"/> Identity Theft                                   |
| <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Fraud/Embezzlement                               |
| <input checked="" type="checkbox"/> Flooding/Water Damage                |   |

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Risk Management                                      | <input checked="" type="checkbox"/> Audit and Accountability          |
| <input checked="" type="checkbox"/> Access Control                                       | <input checked="" type="checkbox"/> Configuration Management          |
| <input checked="" type="checkbox"/> Awareness and Training                               | <input checked="" type="checkbox"/> Identification and Authentication |
| <input checked="" type="checkbox"/> Contingency Planning                                 | <input checked="" type="checkbox"/> Incident Response                 |
| <input checked="" type="checkbox"/> Physical and Environmental Protection                | <input checked="" type="checkbox"/> Media Protection                  |
| <input checked="" type="checkbox"/> Personnel Security                                   |   |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments |   |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer:

The facility Privacy Officer will monitor compliance with privacy policy through various means,including continuous assessment for privacy compliance. (Reference: VHA Handbook 1605.2, Minimum Necessary Standard For Protected Health Information)

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?  
(Choose One)

- ☒ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?  
(Choose One)

- ☒ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?  
(Choose One)

- ☒ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?  
The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

---

Add any additional comments on this tab for any question in the form you want to comment on.  
Please indicate the question you are responding to and then add your comments.

---

(FY 2010) PIA: VBA Minor Applications

---

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System Veterans Assistance Discharge System (VADS)	Education Training Website  VR&E Training Website VA Reserve Educational Assistance Program	Appraisal System Web Electronic Lender Identification
LGY Processing	Web Automated Verification of Enrollment Right Now Web VA Online Certification of Enrollment (VA-ONCE)	CONDO PUD Builder Centralized Property Tracking System Electronic Appraisal System
Loan Service and Claims LGY Home Loans	Automated Folder Processing System (AFPS) Personal Computer Generated Letters (PCGL) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	Web LGY  Access Manager  SAHSHA  VBA Data Warehouse Distribution of Operational Resources (DOOR)
Search Participant Profile (SPP)		
Control of Veterans Records (COVERS)		
SHARE Modern Awards Process Development (MAP-D) Rating Board Automation 2000 (RBA2000)		
		Enterprise Wireless Messaging System (Blackberry) VBA Enterprise Messaging System
State of Case/Supplemental (SOC/SSOC)	SHARE	
Awards	State Benefits Reference System Training and Performance Support System (TPSS) Veterans Appeals Control and Locator System (VACOLS) Veterans On-Line Applications (VONAPP)	LGY Centralized Fax System  Review of Quality (ROQ)  Automated Sales Reporting (ASR)
Financial and Accounting System (FAS)		
Eligibility Verification Report (EVR) Automated Medical Information System (AMIS)290	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Web Automated Reference Material System (WARMS)		
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI) Control of Veterans Records (COVERS)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)		Inventory Management System (IMS)
Fiduciary STAR Case Review Veterans Exam Request Info System (VERIS) Web Automated Folder Processing System (WAFPS)	Fiduciary Beneficiary System (FBS) Hearing Officer Letters and Reports System (HOLAR)  Inforce	Synquest  RAI/MDS  ASSISTS
Courseware Delivery System (CDS) Electronic Performance Support System (EPSS) Veterans Service Representative (VSR) Advisor	Awards  Actuarial  Insurance Self Service	MUSE  Bbraun (CP Hemo)  VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #2	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #3	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

---

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program CH 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

---

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	SUPPORT
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION	KERNEL
AUTOMATED LAB INSTRUMENTS	SYSTEM	KIDS
AUTOMATED MED INFO EXCHANGE	EQUIPMENT/TURN-IN	LAB SERVICE
BAR CODE MED ADMIN	REQUEST	LETTERMAN
BED CONTROL	EVENT CAPTURE	LEXICON UTILITY
BENEFICIARY TRAVEL	EVENT DRIVEN	LIBRARY
CAPACITY MANAGEMENT - RUM	REPORTING	LIST MANAGER
CAPRI	EXTENSIBLE EDITOR	MAILMAN
CAPACITY MANAGEMENT TOOLS	EXTERNAL PEER REVIEW	MASTER PATIENT INDEX
CARE MANAGEMENT	FEE BASIS	VISTA
CLINICAL CASE REGISTRIES	FUNCTIONAL	MCCR NATIONAL
CLINICAL INFO RESOURCE NETWORK	INDEPENDENCE	DATABASE
CLINICAL MONITORING SYSTEM	GEN. MED. REC. - GENERATOR	MEDICINE
CLINICAL PROCEDURES	GEN. MED. REC. - I/O	MENTAL HEALTH
CLINICAL REMINDERS	GEN. MED. REC. - VITALS	MICOM
CMOP	GENERIC CODE SHEET	MINIMAL PATIENT
CONSULT/REQUEST TRACKING	GRECC	DATASET
CONTROLLED SUBSTANCES	HEALTH DATA &	MYHEALTHVET
CPT/HCPCS CODES	INFORMATICS	Missing Patient Reg (Original)
CREDENTIALS TRACKING	HEALTH LEVEL SEVEN	A4EL
DENTAL	HEALTH SUMMARY	NATIONAL DRUG FILE
DIETETICS	HINQ	NATIONAL LABORATORY
DISCHARGE SUMMARY	HOSPITAL BASED HOME	TEST
DRG GROUPER	CARE	NDBI
	ICR - IMMUNOLOGY CASE	NETWORK HEALTH
	REGISTRY	EXCHANGE
	IFCAP	NOIS
	IMAGING	NURSING SERVICE
	INCIDENT REPORTING	OCCURRENCE SCREEN
	INCOME VERIFICATION	ONCOLOGY
	MATCH	ORDER ENTRY/RESULTS
	INCOMPLETE RECORDS	REPORTING
	TRACKING	

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #2	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #3	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

---

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	
PHARMACY BENEFITS	UTILIZATION REVIEW
MANAGEMENT	
PHARMACY DATA	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	
PHARMACY NATIONAL	VA FILEMAN
DATABASE	
PHARMACY PRESCRIPTION	VBECs
PRACTICE	VDEF
POLICE & SECURITY	
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	
QUALITY IMPROVEMENT	VISTALINK SECURITY
CHECKLIST	
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
	ANRV
RADIOLOGY/NUCLEAR	VOLUNTARY TIMEKEEPING
MEDICINE	
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY	
SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF	
TOOL	

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #2	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

Minor app #3	Name		Description		Comments
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

## (FY 2010) PIA: Final Signatures

Facility Name: Hines OI Field Office

Title:	Name:	Phone:	Email:
Privacy Officer:	Sheila Merrier	224-610-3383	<a href="mailto:sheila.merrier2@va.gov">sheila.merrier2@va.gov</a>
Digital Signature Block			
Information Security Officer:	John Rinkema	224-610-3805	<a href="mailto:john.rinkema@va.gov">john.rinkema@va.gov</a>
Digital Signature Block			
Chief Information Officer:	Paul Lam	224-610-5700	<a href="mailto:paul.lam@va.gov">paul.lam@va.gov</a>
Digital Signature Block			
Person Completing Document:	Mayra Acevedo-Negron	561-422-1290	<a href="mailto:mayra.acevedonegron@va.gov">mayra.acevedonegron@va.gov</a>
Digital Signature Block			
System / Application / Program Manager:	n/a	0	0
Digital Signature Block			

Date of Report: 5/7/2010  
OMB Unique Project Identifier JIF# 00-001

Project Name Federal Health Care Center- Inter  
Agency Services (FHCC-IAS)